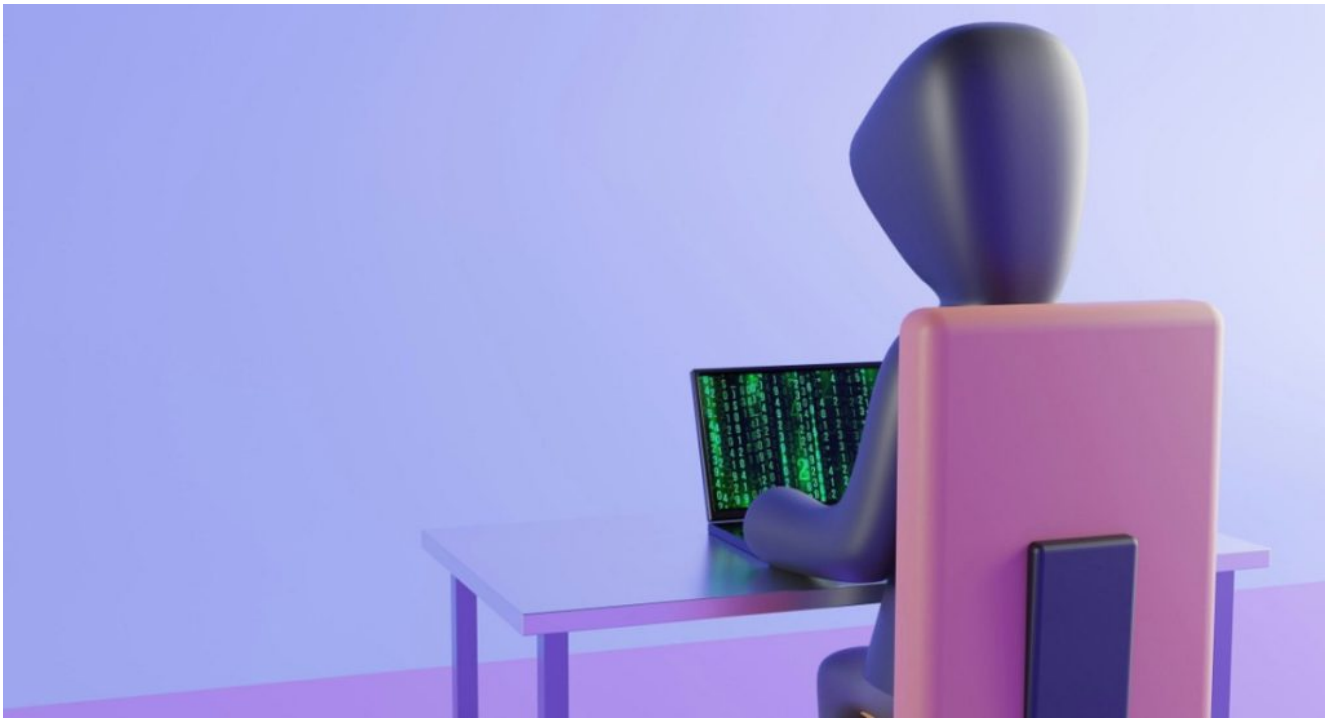
Estafas tecnológicas: cinco claves para detectar cuándo una aplicación es legítima o falsa

14/08/2024



Las **aplicaciones** se convirtieron en una **parte elemental** de los **celulares**, ya sea para comunicarse, entretenerse o solucionar cuestiones de trabajo, entre otras cosas. Y justamente, gracias a estos atractivos, también crecieron los **ciberdelitos**.

En muchas ocasiones, los hackers crean **aplicaciones maliciosas o imitan las legítimas** para robar contraseñas y acceder a cuentas bancarias. Frente a este contexto, **es crucial identificar estas aplicaciones engañosas** para proteger la privacidad.

Hackers; ciberdelito. Foto: Unsplash.

A continuación, te ayudamos con **cinco claves** para evitar ser

una víctima de **estafas tecnológicas** en tiempos de **digitalización**.

Cinco claves para detectar una aplicación falsa

1- Revisiones y calificaciones sospechosas

Antes de descargar una aplicación, es necesario revisar las **calificaciones** y los **comentarios** de otros usuarios. Las apps legítimas suelen tener una cantidad significativa de reseñas, tanto **positivas** como **negativas**. Si una app tiene una calificación inusualmente alta con comentarios que parecen genéricos o repetitivos, es una señal de alerta.

También, es importante prestar atención a las fechas de las reseñas. Si todas las calificaciones positivas se publicaron en un **corto período**, podría ser un indicio de que se están utilizando tácticas engañosas para inflar la reputación de la app.

2- Solicitudes de permisos excesivos

Las aplicaciones legítimas suelen **solicitar permisos** que son necesarios para su funcionamiento. Por ejemplo, una app de cámara necesitará acceso a la cámara y al almacenamiento, mientras que una app de mensajería puede requerir acceso a tus contactos.

Sin embargo, si una aplicación solicita permisos que parecen **innecesarios** para su funcionalidad, es una señal de que podría estar intentando **acceder a información personal** sin justificación.

Hackers; ciberdelito. Foto: Unsplash.

3- Falta de información del desarrollador

Las aplicaciones legítimas suelen ser creadas por desarrolladores conocidos y confiables o grandes empresas tecnológicas, como **Apple**, **Google**, **Meta**, **Microsoft**, entre otras.

Si el desarrollador es una compañía pequeña y desconocida, es necesario verificar su información en la tienda de aplicaciones. Un desarrollador con un **historial sólido y aplicaciones bien valoradas** es más probable que sea legítimo.

4- Errores gramaticales y de diseño

Las aplicaciones fraudulentas a menudo son el resultado de un **desarrollo apresurado o poco profesional**. Si hay errores gramaticales, ortográficos o de diseño en la interfaz de la app, esto puede ser un signo de que no es legítima.

Un diseño poco intuitivo o una interfaz que parece **desorganizada** también pueden ser señales de advertencia. Las aplicaciones bien desarrolladas suelen seguir pautas de usabilidad, lo que facilita la navegación para los usuarios.

5- Promesas demasiado buenas para ser verdaderas

Si una aplicación promete resultados milagrosos, como perder peso rápidamente, ganar dinero fácil o acceder a contenido exclusivo de forma gratuita, es probable que sea una **estafa**. También, hay que desconfiar de las apps que requieren **pagos anticipados** o que ofrecen pruebas gratuitas que después se convierten en **suscripciones costosas**.

Fuente: Canal 26